CLAIMS

1. A method used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

distributing a public key corresponding to the private key;

receiving a secret key encrypted by the public key;

decrypting the secret key by the private key;

receiving the access key encrypted by the secret key; and

decrypting the access key by the secret key.

2. The method of claim 1, wherein the secret key is a registration key.

3. The method of claim 1, wherein the secret key is a temporary key.

4. The method of claim 1, further comprising:

deriving a short key based on the access key;

receiving encrypted broadcast content; and

decrypting the encrypted broadcast content using the short key.

5. A method used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

distributing a public key corresponding to the private key;

receiving the access key encrypted by the public key; and

decrypting the access key by the private key.

6. The method of claim 5, wherein the secret key is a registration key.

7. The method of claim 5, wherein the secret key is a temporary key.

8. The method of claim 5, further comprising:

deriving a short key based on the access key;

receiving encrypted broadcast content; and

decrypting the encrypted broadcast content using the short key.

9. A method used for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

receiving a public key corresponding to a private key;

encrypting the secret key with the public key;

sending the encrypted secret key;

receiving the access key encrypted by the secret key; and

decrypting the access key by the secret key.

10. The method of claim 9, wherein the secret key is a registration key.

11. The method of claim 9, wherein the secret key is a temporary key.

12. The method of claim 9, further comprising:

deriving a short key based on the access key;

receiving encrypted broadcast content; and

decrypting the encrypted broadcast content using the short key.

13. A method used for distributing an access key to provide broadcast services from a content provider comprising:

receiving a public key corresponding to a private key;

encrypting secret key using the public key;

sending the encrypted secret key;

encrypting the access key using the secret key; and

sending the encrypted access key.

14. The method of claim 13, wherein the secret key is a registration key.

15. The method of claim 13, wherein the secret key is a temporary key.

16. A method used for distributing an access key to provide broadcast services from a content provider comprising:

receiving a public key corresponding to a private key;

encrypting the access key using the pubic key; and

sending the encrypted access key.

17. The method of claim 16, wherein the secret key is a registration key.

18. The method of claim 16, wherein the secret key is a temporary key.

19. A method used for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

distributing a public key corresponding to the private key;

receiving a secret key encrypted by the public key;

decrypting the secret key using the private key;

encrypting the access key using the secret key; and

sending the encrypted access key.

20. The method of claim 19, wherein the secret key is a registration key.

21. The method of claim 19, wherein the secret key is a temporary key.

22. Apparatus for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

means for distributing a public key corresponding to the private key;

means for receiving a secret key encrypted by the public key;

means for decrypting the secret key by the private key;

means for receiving the access key encrypted by the secret key; and

means for decrypting the access key by the secret key.

23. The apparatus of claim 22, wherein the secret key is a registration key.

24. The apparatus of claim 22, wherein the secret key is a temporary key.

25. Apparatus for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

means for distributing a public key corresponding to the private key;

means for receiving the access key encrypted by the public key; and

means for decrypting the access key by the private key.

26. The apparatus of claim 25, wherein the secret key is a registration key.

27. The apparatus of claim 25, wherein the secret key is a temporary key.

28. Apparatus for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

means for receiving a public key corresponding to a private key;

means for encrypting the secret key with the public key;

means for sending the encrypted secret key;

means for receiving the access key encrypted by the secret key; and

means for decrypting the access key by the secret key.

29. The apparatus of claim 28, wherein the secret key is a registration key.

30. The apparatus of claim 28, wherein the secret key is a temporary key.

31. Apparatus for distributing an access key to provide broadcast services from a content provider comprising:

means for receiving a public key corresponding to a private key;

means for encrypting secret key using the public key;

means for sending the encrypted secret key;

means for encrypting the access key using the secret key; and

means for sending the encrypted access key.

32. The apparatus of claim 31, wherein the secret key is a registration key.

33. The apparatus of claim 31, wherein the secret key is a temporary key.

34. Apparatus for distributing an access key to provide broadcast services from a content provider comprising:

means for receiving a public key corresponding to a private key;

means for encrypting the access key using the pubic key; and

means for sending the encrypted access key.

35. The apparatus of claim 34, wherein the secret key is a registration key.

36. The apparatus of claim 34, wherein the secret key is a temporary key.

37. Apparatus for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

means for distributing a public key corresponding to the private key;

means for receiving a secret key encrypted by the public key;

means for decrypting the secret key using the private key;

means for encrypting the access key using the secret key; and

means for sending the encrypted access key.

38. The apparatus of claim 37, wherein the secret key is a registration key.

39. The apparatus of claim 37, wherein the secret key is a temporary key.

40. Machine readable medium used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

codes for distributing a public key corresponding to the private key;

codes for receiving a secret key encrypted by the public key;

codes for decrypting the secret key by the private key;

codes for receiving the access key encrypted by the secret key; and

codes for decrypting the access key by the secret key.

41. The medium of claim 40, wherein the secret key is a registration key.

42. The medium of claim 40, wherein the secret key is a temporary key.

43. Machine readable medium used for provisioning an access key to receive broadcast services in a terminal storing a private key comprising:

codes for distributing a public key corresponding to the private key;

codes for receiving the access key encrypted by the public key; and

codes for decrypting the access key by the private key.

44. The medium of claim 43, wherein the secret key is a registration key.

45. The medium of claim 43, wherein the secret key is a temporary key.

46. Machine readable medium used for provisioning an access key to receive broadcast services in a terminal storing a secret key comprising:

codes for receiving a public key corresponding to a private key;

codes for encrypting the secret key with the public key;

codes for sending the encrypted secret key;

codes for receiving the access key encrypted by the secret key; and

codes for decrypting the access key by the secret key.

47. The medium of claim 46, wherein the secret key is a registration key.

48. The medium of claim 46, wherein the secret key is a temporary key.

49. Machine readable medium used for distributing an access key to provide broadcast services from a content provider comprising:

codes for receiving a public key corresponding to a private key;

codes for encrypting secret key using the public key;

codes for sending the encrypted secret key;

codes for encrypting the access key using the secret key; and

codes for sending the encrypted access key.

50. The medium of claim 49, wherein the secret key is a registration key.

51. The medium of claim 49, wherein the secret key is a temporary key.

52. Machine readable medium used for distributing an access key to provide broadcast services from a content provider comprising:

codes for receiving a public key corresponding to a private key;

codes for encrypting the access key using the pubic key; and

codes for sending the encrypted access key.

53. The medium of claim 52, wherein the secret key is a registration key.

54. The medium of claim 52, wherein the secret key is a temporary key.

55. Machine readable medium for distributing an access key to provide broadcast services from a content provider having stored a private key comprising:

codes for distributing a public key corresponding to the private key;

codes for receiving a secret key encrypted by the public key;

codes for decrypting the secret key using the private key;

codes for encrypting the access key using the secret key; and

codes for sending the encrypted access key.

56. The medium of claim 55, wherein the secret key is a registration key.

57. The medium of claim 55, wherein the secret key is a temporary key.